

EXPRESS MAIL LABEL NO:

EV 047 534 011 US

This application is submitted in the name of the following inventors:

| <u>Inventor</u> | <u>Citizenship</u> | <u>Residence City and State</u> |
|--------------------------|--------------------|---------------------------------|
| Bechtolsheim, Andreas V. | Germany | Stanford, California |
| Cheriton, David R. | | |

The assignee is Cisco Technology, Inc., a California corporation having an office at 170 West Tasman Drive, San Jose CA 95134.

Title of the Invention

Access Control List Processing in Hardware

Background of the Invention

1. Field of the Invention

This invention relates to access control list processing.

2. *Related Art*

In a computer network for transmitting information, messages can be restricted from being transmitted from selected source devices to selected destination devices. In known computer networks, this form of restriction is known as "access control" and is performed by routers, which route messages (in the form of individual packets of information) from source devices to destination devices. One known technique for access control is for each router to perform access control by reference to one or more ACLs (access control lists); the ACL describes which selected source devices are permitted (and which denied) to send packets to which selected destination devices.

In a known standard for ACL format, each ACL includes a plurality of access control specifiers, each of which selects a range of sender and destination IP address prefix or subnet, and port, and provides that packet transmission from that selected set of senders to that selected set of destinations is either specifically permitted or specifically denied. ACLs are associated with input interfaces and independently with output interfaces for each router. In known routers such as those manufactured by Cisco Systems, Inc., of San Jose, California, the router is provided with an ACL using an ACL command language, interpreted by operating system software for the router, such as the IOS operating system.

1 One problem in the known art is that processing of packets to enforce ac-
2 cess control according to the ACL is processor-intensive and can therefore be relatively
3 slow, particularly in comparison with desired rates of speed for routing packets. This
4 problem is exacerbated when access control is enforced for packets using software in the
5 router, because software processing of the ACL can be quite slow relative to hardware
6 processing of the packet for routing.

7
8 One known solution is to reduce the number of packets for which access
9 control requires actual access to the ACL. In a technique known as "netflow switching,"
10 packets are identified as belonging to selected "flows," and each packet in a flow is ex-
11 pected to have identical routing and access control characteristics. Therefore, access
12 control only requires reference to the ACL for the first packet in a flow; subsequent pack-
13 ets in the same flow can have access control enforced identically to the first packet, by
14 reference to a routing result cached by the router and used for the entire flow.

15
16 Netflow switching is further described in detail in the following patent ap-
17 plications:

18
19 o U.S. Application Serial No. 08/581,134, titled "Method For Traffic Management,
20 Traffic Prioritization, Access Control, and Packet Forwarding in a Datagram Com-
21 puter Network", filed December 29, 1995, in the name of inventors David R.

Cheriton and Andreas V. Bechtolsheim, assigned to Cisco Technology, Inc., attorney docket number CIS-019;

U.S. Application Serial No. 08/655,429, titled "Network Flow Switching and Flow Data Export", filed May 28, 1996, in the name of inventors Darren Kerr and Barry Bruins, and assigned to Cisco Technology, Inc., attorney docket number CIS-016; and

U.S. Application Serial No. 08/771,438, titled "Network Flow Switching and Flow Data Export", filed December 20, 1996, in the name of inventors Darren Kerr and Barry Bruins, assigned to Cisco Technology, Inc., attorney docket number CIS-017.

These patent applications are collectively referred to herein as the "Netflow Switching Disclosures". Each of these applications is hereby incorporated by reference as if fully set forth herein.

While netflow switching achieves the goal of improving the speed of enforcing access control by the router, it still has the drawback that comparing at least some incoming packets against the ACL must be performed using software. Thus, the relative slowness required by software processing of the ACL is not completely avoided.

Summary of the Invention

The invention provides a method and system for hardware processing of ACLs and thus hardware enforcement of access control. A sequence of access control specifiers from an ACL are recorded in a CAM, and information from the packet header is used to attempt to match selected source and destination IP addresses or subnets, ports, and protocols, against all the ACL specifiers at once. Successful matches are input to a priority selector, which selects the match with the highest priority (that is, the match that is first in the sequence of access control specifiers). The specified result of the selected match is used to permit or deny access for the packet without need for software processing, preferably at a rate comparable to wirespeed.

In a preferred embodiment, the CAM includes an ordered sequence of entries, each of which has an array of ternary elements for matching on logical "0", logical "1", or on any value, and each of which generates a match signal. The ACL entered for recording in the CAM can be optimized to reduce the number of separate entries in the CAM, such as by combining entries which are each special cases of a more general access control specifier.

A router including the CAM can also include preprocessing circuits for certain range comparisons which have been found both to be particularly common and to be otherwise inefficiently represented by the ternary nature of the CAM. For example,

comparisons of the port number against known special cases, such as “greater than 1023” and “within the range 6000 to 6500”, can be treated by circuitry for performing range comparisons or by reference to one or more auxiliary CAMs.

The invention can also be used to augment or override routing decisions otherwise made by the router, so as to implement QOS (quality of service), and other administrative policies, using the CAM.

Brief Description of the Drawings

Figure 1 shows a block diagram of a system for access control list processing.

Figure 2 shows a block diagram of an access control element.

Figure 3 shows a flow diagram of a method for access control list processing in hardware.

Detailed Description of the Preferred Embodiment

In the following description, a preferred embodiment of the invention is described with regard to preferred process steps and data structures. Those skilled in the art

would recognize after perusal of this application that embodiments of the invention can be implemented using circuits adapted to particular process steps and data structures described herein, and that implementation of the process steps and data structures described herein would not require undue experimentation or further invention.

System Elements

Figure 1 shows a block diagram of a system for access control list processing.

A system 100 includes a set of packet input interfaces 101, a routing element 110, an access control element 120, and a set of packet output interfaces 102. The system 100 receives packets 130 at the input interfaces 101; each packet 130 indicates a source device 131, from which it was sent, and a destination device 132, to which it is intended to go. The routing element 110 processes each packet 130 to select one or more of the output interfaces 102 to which the packet 130 should be forwarded. The access control element 120 determines if the packet 130 has permission to be forwarded from its source device 131 to its destination device 132. Each packet 130 that has permission to be forwarded is output to its selected output interfaces 102.

1 In a first set of alternative embodiments, the system 100 may include a plu-
2 rality of access control elements 120 operating in parallel in place of the single access
3 control element 120.

4
5 In a second set of alternative embodiments, the system 100 may include one
6 or more access control elements 120 coupled to the input interfaces 101 and operating to
7 determine if packets 130 have permission to be forwarded from their source devices 131
8 at all. The access control element 120 is shown coupled to the routing element 110 to
9 perform access control after a routing decision has been made. However, the access con-
10 trol element 120 is still capable of denying access to packets 130 responsive to whether
11 they have permission to be forwarded from their source devices 131 at all.

12
13 In a third set of alternative embodiments, the system 100 may include one
14 or more access control elements 120 coupled to individual input interfaces 101 and oper-
15 ating to make access control determinations for packets 130 arriving at particular input
16 interfaces 101. Similarly, the system 100 may include one or more access control ele-
17 ments 120 coupled to individual output interfaces 102 and operating to make access con-
18 trol determinations for packets 130 forwarded to particular output interfaces 102.

19
20 *Access Control Element*

21
22 Figure 2 shows a block diagram of an access control element.

1
2 In a preferred embodiment, the access control element 120 operates on a set
3 of selected elements of a packet header 133 for each packet 130. The system 100 collects
4 the selected elements into a packet label 200.

5
6 In a preferred embodiment using netflow switching, the packet label 200
7 used for access control at the input interfaces 101 includes a source device 131, the desti-
8 nation device 132, a port identifier for a port at the source device 131, a port identifier for
9 a port at the destination device 132, and a protocol type. In alternative embodiments, the
10 packet label 200 may be any collection of information derived from the packet 130 (prefer-
11 ably from the packet header 133) used for access control.

12
13 The concept of preprocessing the packet label has wide applicability, in-
14 cluding determining other routing information in response to data in the packet header.
15 For example, in addition to or instead of comparing data in the packet header against
16 known special cases, such as "greater than 1023" and "within the range 6000 to 6500,"
17 preprocessing can include performing logical or arithmetic operations on data in the
18 packet header. Preprocessing can also include data lookup, or substituting new data, in
19 response to data in the packet header.

1 The access control element 120 includes an input port 201 coupled to the
2 packet label 200, an access control memory 210, a priority encoder 220, and an output
3 port 202 coupled to the priority encoder 220.

4
5 When the access control element 120 is disposed for controlling access for
6 packets responsive to their input interfaces 101, the packet label 200 includes an identifier
7 for the input interface 101. When the access control element 120 is disposed for control-
8 ling access for packets responsive to their output interfaces 102, the packet label 200 in-
9 cludes an identifier for the output interface 102.

10
11 The access control memory 210 includes a CAM (content-addressable
12 memory) having a sequence of access control specifiers 211. Each access control speci-
13 fier 211 includes a label match mask 212 and a label match pattern 213. For each access
14 control specifier 211, each bit of the label match mask 212 determines whether or not a
15 corresponding bit of the packet label 200 is tested. If so, the corresponding bit of the la-
16 bel match pattern 213 is compared for equality with the corresponding bit of the packet
17 label 200. If all compared bits are equal, the access control specifier 211 matches the
18 packet label 200. Bits that are not compared have no effect on whether the access control
19 specifier 211 is considered to match the packet label 200 or not.

20
21 The priority encoder 220 is coupled to all of the access control specifiers
22 211, and receives an indicator from each one whether or not that access control specifier

1 211 matched the packet label 200. The priority encoder 220 selects the single access
2 control specifier 211 with the highest priority (in a preferred embodiment, the one with
3 the lowest address in the access control memory 210) and provides an indicator of that
4 single access control specifier 211 to the output port 202.

5
6 The indicator provided to the output port 202 specifies whether or not the
7 packet 130 has permission to be forwarded from its specified source device 131 to its
8 specified destination device 132. In a preferred embodiment, the indicator specifies one
9 of three possibilities: (a) the packet 130 is forwarded to its calculated output interface and
10 on to its specified destination device 132; (b) the packet 130 is dropped; or (c) the packet
11 130 is forwarded to a "higher-level" processor for further treatment. When a packet 130
12 is dropped it is effectively denied access from its specified source device 131 to its speci-
13 fied destination device 132.

14
15 The higher-level processor includes a general-purpose processor, program
16 and data memory, and mass storage, executing operating system and application software
17 for software (rather than hardware) examination of the packet 130. The packet 130 is
18 compared, possibly to the access control specifiers 211 and possibly to other administra-
19 tive policies or restrictions, by the higher-level processor. The higher-level processor
20 specifies whether the packet 130, after processing by the higher-level processor, is for-
21 warding to a selected output interface or is dropped.

Access Control Lists

A Cisco access control list includes a sequence of access control entries, which are mapped to a set of access control specifiers 211. Each access control entry has a structure according to the following syntax:

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny|permit} protocol source source-wildcard [operator port [port]] destination
destination-wildcard [operator port [port]] [established] [precedence precedence]
[tos tos] [log]
```

This syntax, its meaning, and access control entries in general, are further described in documentation for Cisco IOS software, available from Cisco Systems, Inc., in San Jose, California, and hereby incorporated by reference as if fully set forth herein.

Access control entries can specify that particular actions are permitted, denied, or that they will be recorded in a log. Access control entries are interpreted sequentially. Thus, an earlier more specific access control entry can prohibit particular actions (such as receiving messages from a particular sending device), while a later more general access control entry can permit the same actions for other devices (such as other sending devices in the same network).

1 When an access control list is translated for entry into the access control
2 memory, it is optimized to reduce the number of separate entries that are used. Thus, an
3 access control list with N separate access control entries is translated into a set of access
4 control specifiers 211 that can be smaller or larger than N, depending on the effect of op-
5 timization.

6
7 A first optimization detects separate access control entries that each refer to
8 a special case of a more general access control specifier 211, such as in one of the fol-
9 lowing cases:

10
11 o A first access control entry provides a selected permission for a selected source
12 device 131 2S, and a second access control entry provides the same permission for
13 a selected source device 131 2S+1. The first and second access control entries can
14 be translated into a single more general access control specifier 211 with an un-
15 matched bit in the 2^0 position.

16
17 o A set of access control entries each provides the same selected permission for a
18 range of selected source devices 131 S through T, and the range S through T can
19 be represented as a smaller number of bit strings with unmatched bits.

20
21 o A set of access control entries provides a selected permission for a comparison of
22 source device 131 addresses with a test value V.

1
2 A second optimization detects range comparisons that have been found to
3 be particularly common. For example, it is common to compare the source or destination
4 port number for being greater than 1023, or for being within the range 6000 to 6500. To
5 compare the source or destination port number for being greater than 1023 with matched
6 and unmatched bits would use about six entries for each such comparison (to test each
7 one of the six high-order bits of the port number for being logical "1").
8

9 In a preferred embodiment, a comparison circuit 230 compares the source
10 port number and the destination port number with these known ranges and provides a set
11 of comparison bits 231 indicating whether or not the source port number and the destina-
12 tion port number are within each specified range. The comparison circuit 230 includes a
13 finite state machine 232 (or other element) for storing lower and upper bounds for each
14 specified range. The comparison bits 231 are coupled to the input port 201 of the access
15 control element 120 for treatment as matchable input bits supplemental to the header of
16 the packet 130.
17

18 In various embodiments, the invention can be used to augment or override
19 routing decisions otherwise made by the router, using the access control element 120. In
20 addition to specifying that the packet 130 is to be dropped or forwarded to the higher-
21 level processor, the access control element 120 can alter the output interface, which was
22 selected by the routing element 110, to another selected output interface. The invention

1 can thus be used to implement QOS (quality of service) policies and other administrative
2 policies.

3
4 *Method of Operation*

5
6 Figure 3 shows a flow diagram of a method for access control list process-
7 ing in hardware.

8
9 A method 300 includes a set of flow points to be noted, and steps to be exe-
10 cuted, cooperatively by the elements of the system 100.

11
12 At a flow point 310, a packet is received at one of the packet input inter-
13 faces 101.

14
15 At a step 321, the routing element 110 receives an input packet 130.

16
17 At a step 322, the routing element 110 identifies the header for the packet
18 130.

19
20 At a step 323, the routing element 110 selects portions of the header for use
21 as the packet label 200 for access control. In a preferred embodiment, the packet label
22 200 used for access control at the input interfaces 101 includes the source device 131, the

destination device 132, the port identifier at the source device 131, the port identifier at the destination device 132, and a protocol type.

At a step 324, the routing element 110 couples the packet label 200 and an input interface specifier to the input access control element 120.

At a step 325, the routing element 110 determines a selected output interface for the packet 130.

At a step 326, preferably performed in parallel with the step 325, the input access control element 120 determines the input permission for the packet 130, that is, whether the routing element 110 permits forwarding the packet 130 from the source device 131 for the packet 130.

The step 326 includes matching the packet label 200 against the access control memory 210 for the input access control element 120, determining all of the successful matches, coupling the successful matches to the priority encoder 220 for the input access control element 120, determining the highest-priority match, and providing an output result from the input access control element 120.

If at the step 326, the input access control element 120 determines that the higher-level processor should process the packet 130, the higher-level processor proc-

esses the packet 130. A result from the higher-level processor is substituted for the result from the input access control element 120.

If at the step 326, the input access control element 120 (or the higher-level processor) determines that the packet 130 should be dropped, the packet 130 is dropped, and the routing element 110 takes no further action with regard to the packet 130.

At a step 327, the routing element 110 couples the packet label 200 and the output interface specifier to the output access control element 120.

At a step 328, the output access control element 120 determines the output permission for the packet 130, that is, whether the routing element 110 permits forwarding the packet 130 to the destination device 132 for the packet 130.

The step 326 includes the following actions:

- o matching the packet label 200 against the access control memory 210 for the output access control element 120;
- o determining all of the successful matches;

- o coupling the successful matches to the priority encoder 220 for the output access control element 120;
- o determining the highest-priority match; and
- o providing an output result from the output access control element 120.

If at the step 328, the output access control element 120 determines that the higher-level processor should process the packet 130, the higher-level processor processes the packet 130. A result from the higher-level processor is substituted for the result from the output access control element 120.

If at the step 328, the output access control element 120 (or the higher-level processor) determines that the packet 130 should be dropped, the packet 130 is dropped, and the routing element 110 takes no further action with regard to the packet 130.

At a flow point 330, the packet is ready for transmission to one of the packet output interfaces 102.

1 *Alternative Embodiments*

2

3 Although preferred embodiments are disclosed herein, many variations are
 4 possible which remain within the concept, scope, and spirit of the invention, and these
 5 variations would become clear to those skilled in the art after perusal of this application.

1000
 9999
 9998
 9997
 9996
 9995
 9994
 9993
 9992
 9991
 9990
 9989
 9988
 9987
 9986
 9985
 9984
 9983
 9982
 9981
 9980
 9979
 9978
 9977
 9976
 9975
 9974
 9973
 9972
 9971
 9970
 9969
 9968
 9967
 9966
 9965
 9964
 9963
 9962
 9961
 9960
 9959
 9958
 9957
 9956
 9955
 9954
 9953
 9952
 9951
 9950
 9949
 9948
 9947
 9946
 9945
 9944
 9943
 9942
 9941
 9940
 9939
 9938
 9937
 9936
 9935
 9934
 9933
 9932
 9931
 9930
 9929
 9928
 9927
 9926
 9925
 9924
 9923
 9922
 9921
 9920
 9919
 9918
 9917
 9916
 9915
 9914
 9913
 9912
 9911
 9910
 9909
 9908
 9907
 9906
 9905
 9904
 9903
 9902
 9901
 9900
 9899
 9898
 9897
 9896
 9895
 9894
 9893
 9892
 9891
 9890
 9889
 9888
 9887
 9886
 9885
 9884
 9883
 9882
 9881
 9880
 9879
 9878
 9877
 9876
 9875
 9874
 9873
 9872
 9871
 9870
 9869
 9868
 9867
 9866
 9865
 9864
 9863
 9862
 9861
 9860
 9859
 9858
 9857
 9856
 9855
 9854
 9853
 9852
 9851
 9850
 9849
 9848
 9847
 9846
 9845
 9844
 9843
 9842
 9841
 9840
 9839
 9838
 9837
 9836
 9835
 9834
 9833
 9832
 9831
 9830
 9829
 9828
 9827
 9826
 9825
 9824
 9823
 9822
 9821
 9820
 9819
 9818
 9817
 9816
 9815
 9814
 9813
 9812
 9811
 9810
 9809
 9808
 9807
 9806
 9805
 9804
 9803
 9802
 9801
 9800
 9799
 9798
 9797
 9796
 9795
 9794
 9793
 9792
 9791
 9790
 9789
 9788
 9787
 9786
 9785
 9784
 9783
 9782
 9781
 9780
 9779
 9778
 9777
 9776
 9775
 9774
 9773
 9772
 9771
 9770
 9769
 9768
 9767
 9766
 9765
 9764
 9763
 9762
 9761
 9760
 9759
 9758
 9757
 9756
 9755
 9754
 9753
 9752
 9751
 9750
 9749
 9748
 9747
 9746
 9745
 9744
 9743
 9742
 9741
 9740
 9739
 9738
 9737
 9736
 9735
 9734
 9733
 9732
 9731
 9730
 9729
 9728
 9727
 9726
 9725
 9724
 9723
 9722
 9721
 9720
 9719
 9718
 9717
 9716
 9715
 9714
 9713
 9712
 9711
 9710
 9709
 9708
 9707
 9706
 9705
 9704
 9703
 9702
 9701
 9700
 9699
 9698
 9697
 9696
 9695
 9694
 9693
 9692
 9691
 9690
 9689
 9688
 9687
 9686
 9685
 9684
 9683
 9682
 9681
 9680
 9679
 9678
 9677
 9676
 9675
 9674
 9673
 9672
 9671
 9670
 9669
 9668
 9667
 9666
 9665
 9664
 9663
 9662
 9661
 9660
 9659
 9658
 9657
 9656
 9655
 9654
 9653
 9652
 9651
 9650
 9649
 9648
 9647
 9646
 9645
 9644
 9643
 9642
 9641
 9640
 9639
 9638
 9637
 9636
 9635
 9634
 9633
 9632
 9631
 9630
 9629
 9628
 9627
 9626
 9625
 9624
 9623
 9622
 9621
 9620
 9619
 9618
 9617
 9616
 9615
 9614
 9613
 9612
 9611
 9610
 9609
 9608
 9607
 9606
 9605
 9604
 9603
 9602
 9601
 9600
 9599
 9598
 9597
 9596
 9595
 9594
 9593
 9592
 9591
 9590
 9589
 9588
 9587
 9586
 9585
 9584
 9583
 9582
 9581
 9580
 9579
 9578
 9577
 9576
 9575
 9574
 9573
 9572
 9571
 9570
 9569
 9568
 9567
 9566
 9565
 9564
 9563
 9562
 9561
 9560
 9559
 9558
 9557
 9556
 9555
 9554
 9553
 9552
 9551
 9550
 9549
 9548
 9547
 9546
 9545
 9544
 9543
 9542
 9541
 9540
 9539
 9538
 9537
 9536
 9535
 9534
 9533
 9532
 9531
 9530
 9529
 9528
 9527
 9526
 9525
 9524
 9523
 9522
 9521
 9520
 9519
 9518
 9517
 9516
 9515
 9514
 9513
 9512
 9511
 9510
 9509
 9508
 9507
 9506
 9505
 9504
 9503
 9502
 9501
 9500
 9499
 9498
 9497
 9496
 9495
 9494
 9493
 9492
 9491
 9490
 9489
 9488
 9487
 9486
 9485
 9484
 9483
 9482
 9481
 9480
 9479
 9478
 9477
 9476
 9475
 9474
 9473
 9472
 9471
 9470
 9469
 9468
 9467
 9466
 9465
 9464
 9463
 9462
 9461
 9460
 9459
 9458
 9457
 9456
 9455
 9454
 9453
 9452
 9451
 9450
 9449
 9448
 9447
 9446
 9445
 9444
 9443
 9442
 9441
 9440
 9439
 9438
 9437
 9436
 9435
 9434
 9433
 9432
 9431
 9430
 9429
 9428
 9427
 9426
 9425
 9424
 9423
 9422
 9421
 9420
 9419
 9418
 9417
 9416
 9415
 9414
 9413
 9412
 9411
 9410
 9409
 9408
 9407
 9406
 9405
 9404
 9403
 9402
 9401
 9400
 9399
 9398
 9397
 9396
 9395
 9394
 9393
 9392
 9391
 9390
 9389
 9388
 9387
 9386
 9385
 9384
 9383
 9382
 9381
 9380
 9379
 9378
 9377
 9376
 9375
 9374
 9373
 9372
 9371
 9370
 9369
 9368
 9367
 9366
 9365
 9364
 9363
 9362
 9361
 9360
 9359
 9358
 9357
 9356
 9355
 9354
 9353
 9352
 9351
 9350
 9349
 9348
 9347
 9346
 9345
 9344
 9343
 9342
 9341
 9340
 9339
 9338
 9337
 9336
 9335
 9334
 9333
 9332
 9331
 9330
 9329
 9328
 9327
 9326
 9325
 9324
 9323
 9322
 9321
 9320
 9319
 9318
 9317
 9316
 9315
 9314
 9313
 9312
 9311
 9310
 9309
 9308
 9307
 9306
 9305
 9304
 9303
 9302
 9301
 9300
 9299
 9298
 9297
 9296
 9295
 9294
 9293
 9292
 9291
 9290
 9289
 9288
 9287
 9286
 9285
 9284
 9283
 9282
 9281
 9280
 9279
 9278
 9277
 9276
 9275
 9274
 9273
 9272
 9271
 9270
 9269
 9268
 9267
 9266
 9265
 9264
 9263
 9262
 9261
 9260
 9259
 9258
 9257
 9256
 9255
 9254
 9253
 9252
 9251
 9250
 9249
 9248
 9247
 9246
 9245
 9244
 9243
 9242
 9241
 9240
 9239
 9238
 9237
 9236
 9235
 9234
 9233
 9232
 9231
 9230
 9229
 9228
 9227
 9226
 9225
 9224
 9223
 9222
 9221
 9220
 9219
 9218
 9217
 9216
 9215
 9214
 9213
 9212
 9211
 9210
 9209
 9208
 9207
 9206
 9205
 9204
 9203
 9202
 9201
 9200
 9199
 9198
 9197
 9196
 9195
 9194
 9193
 9192
 9191
 9190
 9189
 9188
 9187
 9186
 9185
 9184
 9183
 9182
 9181
 9180
 9179
 9178
 9177
 9176
 9175
 9174
 9173
 9172
 9171
 9170
 9169
 9168
 9167
 9166
 9165
 9164
 9163
 9162
 9161
 9160
 9159
 9158
 9157
 9156
 9155
 9154
 9153
 9152
 9151
 9150
 9149
 9148
 9147
 9146
 9145
 9144
 9143
 9142
 9141
 9140
 9139
 9138
 9137
 9136
 9135
 9134
 9133
 9132
 9131
 9130
 9129
 9128
 9127
 9126
 9125
 9124
 9123
 9122
 9121
 9120
 9119
 9118
 9117
 9116
 9115
 9114
 9113
 9112
 9111
 9110
 9109
 9108
 9107
 9106
 9105
 9104
 9103
 9102
 9101
 9100
 9099
 9098
 9097
 9096
 9095
 9094
 9093
 9092
 9091
 9090
 9089
 9088
 9087
 9086
 9085
 9084
 9083
 9082
 9081
 9080
 9079
 9078
 9077
 9076
 9075
 9074
 9073
 9072
 9071
 9070
 9069
 9068
 9067
 9066
 9065
 9064
 9063
 9062
 9061
 9060
 9059
 9058
 9057
 9056
 9055
 9054
 9053
 9052
 9051
 9050
 9049
 9048
 9047
 9046
 9045
 9044
 9043
 9042
 9041
 9040
 9039
 9038
 9037
 9036
 9035
 9034
 9033
 9032
 9031
 9030
 9029
 9028
 9027
 9026
 9025
 9024
 9023
 9022
 9021
 9020
 9019
 9018
 9017
 9016
 9015
 9014
 9013
 9012
 9011
 9010
 9009
 9008
 9007
 9006
 9005
 9004
 9003
 9002
 9001
 9000
 8999
 8998
 8997
 8996
 8995
 8994
 8993
 8992
 8991
 8990
 8989
 8988
 8987
 8986
 8985
 8984
 8983
 8982
 8981
 8980
 8979
 8978
 8977
 8976
 8975
 8974
 8973
 8972
 8971
 8970
 8969
 8968
 8967
 8966
 8965
 8964
 8963
 8962
 8961
 8960
 8959
 8958
 8957
 8956
 8955
 8954
 8953
 8952
 8951
 8950
 8949
 8948
 8947
 8946
 8945
 8944
 8943
 8942
 8941
 8940
 8939
 8938
 8937
 8936
 8935
 8934
 8933
 8932
 8931
 8930
 8929
 8928
 8927
 8926
 8925
 8924
 8923
 8922
 8921
 8920
 8919
 8918
 8917
 8916
 8915
 8914
 8913
 8912
 8911
 8910
 8909
 8908
 8907
 8906
 8905
 8904
 8903
 8902
 8901
 8900
 8899
 8898
 8897
 8896
 8895
 8894
 8893
 8892
 8891
 8890
 8889
 8888
 8887
 8886
 8885
 8884
 8883
 8882
 8881
 8880
 8879
 8878
 8877
 8876
 8875
 8874
 8873
 8872
 8871
 8870
 8869
 8868
 8867
 8866
 8865
 8864
 8863
 8862
 8861
 8860
 8859
 8858
 8857
 8856
 8855
 8854
 8853
 8852
 8851
 8850
 8849
 8848
 8847
 8846
 8845
 8844
 8843
 8842
 8841
 8840
 8839
 8838
 8837
 8836
 8835
 8834
 8833
 8832
 8831
 8830
 8829
 8828
 8827
 8826
 8825
 8824
 8823
 8822
 8821
 8820
 8819
 8818
 8817
 8816
 8815
 8814
 8813
 8812
 8811
 8810
 8809
 8808
 8807
 8806
 8805
 8804
 8803
 8802
 8801
 8800
 8799
 8798
 8797
 8796
 8795
 8794
 8793
 8792
 8791
 8790
 8789
 8788
 8787
 8786
 8785
 8784
 8783
 8782
 8781
 8780
 8779
 8778
 8777
 8776
 8775
 8774
 8773
 8772
 8771
 8770
 8769
 8768
 8767
 8766
 8765
 8764
 8763
 8762
 8761
 8760
 8759
 8758
 8757
 8756
 8755
 8754
 8753
 8752
 8751
 8750
 8749
 8748
 8747
 8746
 8745
 8744
 8743
 8742
 8741
 8740
 8739
 8738
 8737
 8736
 8735
 8734
 8733
 8732
 8731
 8730
 8729
 8728
 8727
 8726
 8725
 8724
 8723
 8722
 8721
 8720
 8719
 8718
 8717
 8716
 8715
 8714
 8713
 8712
 8711
 8710
 8709
 8708
 8707
 8706
 8705
 8704
 8703
 8702
 8701
 8700
 8699
 8698
 8697
 8696
 8695
 8694
 8693
 8692
 8691
 8690
 8689
 8688
 8687
 8686
 8685
 8684
 8683
 8682
 8681
 8680
 8679
 8678
 8677
 8676
 8675
 8674
 8673
 8672
 8671
 8670
 8669
 8668
 8667
 8666
 8665
 8664
 8663
 8662
 8661
 8660
 8659
 8658
 8657
 8656
 8655
 8654
 8653